IN THE CLAIMS

Please amend the claims to read as follows:

Listing of Claims

1. (Currently Amended) A data processing system for initially generating and installing at least one personal security device PSD master key replacement key and at least one PSD master key inside at least one PSD, said system comprising:

a first server including a data storage ~~means~~ section, wherein said first server is functionally connected to a first hardware security module HSM and a PSD writer;

said PSD writer functionally connected to said first server and said at least one PSD;

said at least one PSD including a non-mutable unique identification number to be sent to said first HSM, a security executive, a first high level key slot and a second high level key slot, wherein said PSD is functionally connected to said PSD writer;

said first HSM including at least one stored public key, at least one stored master key data block, at least one stored master key replacement key data block and a random number generator that generates a random number ~~means for generating~~

~~random numbers~~, wherein said first HSM is functionally connected to said first server;

said first HSM comprising a first diversification section that uses said random number to diversify said master key replacement key data block, which generates a unique key replacement key associated with said non-mutable unique identification number.

2-4. (Canceled).

5. (Currently Amended) The system according to claim ~~3~~ 1, wherein said HSM comprises an encrypting ~~means for encrypting~~ section that encrypts said random number using said at least one stored public key, which generates a unique cryptogram associated with said non-mutable unique identification number.

6. (Original) The system according to claim 5, wherein said unique cryptogram is stored on said first server.

7. (Currently Amended) The system according to claim ~~2~~ 1, wherein said random number is deleted inside said first HSM.

8. (Currently Amended) The system according to claim ~~3~~ 1, comprising a first transfer ~~means for transferring~~ section that transfers to said PSD writer and ~~injecting~~ injects into said at least one PSD said unique key replacement key.

9. (Original) The system according to claim 8, wherein said unique key replacement key is registered with said security executive and installed in said first high level key slot.

10. (Original) The system according to claim 9, wherein said unique key replacement key is registered with said security executive and installed in said second high level key slot.

11. (Currently Amended) The system according to claim ~~2~~ 1, wherein said HSM comprises a second diversification ~~means using~~ section that uses said unique identification number to diversify said at least one stored master key data block, which generates a unique master key.

12. (Original) The system according to claim 11, comprising a second transfer ~~means for transferring~~ section that

transfers to said PSD writer and ~~injecting~~ injects into said at least one PSD said unique master key.

13. (Original) The system according to claim 12, wherein said unique master key is registered with said security executive and installed in said second high level key slot.

14. (Original) The system according to claim 13, wherein said unique master key is registered with said security executive and installed in said first high level key slot.

15. (Currently Amended) A data processing system for post issuance master key replacement for at least one personal security device (PSD), said system comprising:

a client functionally connected to said at least one PSD and in secure communications with a first server;

said at least one PSD including a non-mutable unique identification number, a pre-installed key replacement key, an active master key and a security executive, wherein said PSD is functionally connected to said client;

a first server including at least one stored unique cryptogram associated with said non-mutable unique identification

number, wherein said first server is functionally connected to a first hardware security module HSM and in secure communications with said client;

a second server functionally connected to a second HSM;

said first HSM including ~~cryptography means~~ a cryptographic section, a key generation and key transfer ~~means~~ section, wherein said first HSM is functionally connected to said first server;

said second HSM including ~~cryptography means~~ a cryptographic section, a master key replacement key data block, a master key data block, a key generation and key transfer ~~means~~ section, at least one stored private key, wherein said second HSM is functionally connected to said second server;

a first transfer section that securely transfers said master key replacement key data block, said master key data block, and said at least one stored private key from said second HSM to said first HSM;

a second transfer section that transfers said non-mutable unique identification number to said first server and a retrieving section that retrieves said at least one stored unique cryptogram corresponding to said non-mutable unique identification number;

a third transfer section that transfers said at least one stored unique cryptogram and said non-mutable unique identification number from said first server to said first HSM;

a decrypting section that uses said at least one stored private key to decrypt said at least one stored unique cryptogram, resulting in a random number specific to said at least one PSD; and

a first diversification section that uses said random number to diversify said master key replacement key data block, generating a master key replacement key specific to said at least one PSD.

16-20. (Canceled).

21. (Currently Amended) The system according to claim ~~18~~ 15, comprising a second diversification ~~means using~~ section that uses said non-mutable unique identification number to diversify said master key data block, generating a new master key specific to said at least one PSD.

22. (Currently Amended) The system according to claim ~~20~~ 15, comprising a fourth transfer ~~means for~~ section that securely

~~transferring~~ transfers said master key replacement key to said PSD and said security executive comprises a comparison ~~means for comparing~~ section that compares said master key replacement key to said pre-installed key replacement key.

23. (Original) The system according to claim 22, comprising an unlocking ~~means for unlocking~~ section that unlocks said security executive upon a match between said master key replacement key and said pre-installed key replacement key.

24. (Original) The system according to claim 23, wherein said active master key is deleted from said at least one PSD.

25. (Original) The system according to claim 24, comprising a ~~means for securely transferring~~ transfer section that securely transfers said new master key, ~~installing~~ installs said new master key inside said at least one PSD and ~~registering~~ registers said new master key with said security executive ~~said new master key~~.

26. (Original) The system according to claim 25, comprising a ~~means for relocking~~ section that relocks said security executive following installation of said new master key.

27. (Currently Amended) The system according to claim ~~16~~ 15, wherein said secure transfer occurs at said second server.

28. (Original) The system according to claim 27, wherein said secure transfer occurs at said first server.

29. (Currently Amended) A method for initially generating and installing a master key replacement key and a master key for at least one personal security device (PSD), said method comprising:

receiving a unique PSD identification number by a first data processing device,

generating a master key data block, a master key replacement key data block and asymmetric key pair by a second data processing device,

transferring said master key data block, said master key replacement key data block and a public key of said asymmetric

key pair from said second data processing device to said first data processing device,

generating a random number by said first data processing device,

diversifying said master key replacement data block using said random number and generating a replacement key by said first data processing device,

encrypting said random number with said public key, forming a cryptogram by said first data processing device,

associating said cryptogram with said unique PSD identification number by said first data processing device,

storing said cryptogram by said first data processing device,

deleting said random number from said first data processing device,

diversifying said master key data block using said unique PSD identification number and generating a master key by said first data processing device,

operatively installing said master key replacement key and said master key inside said at least one PSD by said first data processing device.

30. (Original) The method according to claim 29, wherein said first data processing device is an access server.

31. (Original) The method according to claim 30, wherein said first data processing device is a first hardware security module HSM functionally connected to said access server.

32. (Original) The method according to claim 29, wherein said second data processing device is a key management server.

33. (Original) The method according to claim 32, wherein said second data processing device is a second hardware security module HSM functionally connected to said key management server.

34. (Original) The method according to claim 33, wherein said second data processing device is said second HSM functionally connected to said access server.

35. (Currently Amended) A method for post issuance master key replacement for at least one personal security device (PSD), said method comprising:

receiving a unique PSD identification number by a first data processing device,

generating a new master key data block, a master key replacement key data block by a second data processing device,

transferring said new master key data block, said master key replacement key data block and a private key from said second data processing device to said first data processing device,

cross-referencing said unique PSD identification number with a stored cryptogram associated with said at least one PSD by said first data processing device,

retrieving and decrypting said cross-referenced cryptogram using said private key, forming a random number,

diversifying said master key replacement data block using said random number and generating a master key replacement key by said first data processing device,

diversifying said master key data block using said unique PSD identification number and generating a new master key by said first data processing device,

establishing a secure channel with said at least one PSD by said first data processing device,

unlocking a security executive associated with said at least one PSD, using said master key replacement key by said first data processing device,

deleting an existing master key by said first data processing device,

installing said new master key by said first data processing device,

relocking said security executive by said first data processing device,

releasing said secure channel to said at least one PSD by said first data processing device.

36. (Original) The method according to claim 35, wherein said first data processing device is an access server.

37. (Original) The method according to claim 36, wherein said first data processing device is a first hardware security module HSM functionally connected to said access server.

38. (Original) The method according to claim 35, wherein said second data processing device is a key management server.

39. (Original) The method according to claim 38, wherein said second data processing device is a second hardware security module HSM functionally connected to said key management server.

40. (Original) The method according to claim 39, wherein said second data processing device is said second HSM functionally connected to said access server.